

M2047-5
T. KATSURA
H. INOUE

#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出 願 年 月 日
Date of Application:

1999年 9月22日

願 番 号
Application Number:

平成11年特許願第268828号

願 人
Applicant(s):

松下電器産業株式会社

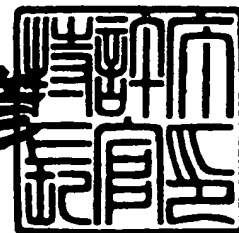
10825 U.S. PTO
09/661276
09/14/00

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 6月23日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3046782

【書類名】 特許願
 【整理番号】 2038610019
 【提出日】 平成11年 9月22日
 【あて先】 特許庁長官殿
 【国際特許分類】 G09F 19/00
 G09C 5/00
 H04N 1/387

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 桂 卓史

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 井上 尚

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097179

【弁理士】

【氏名又は名称】 平野 一幸

【手数料の表示】

【予納台帳番号】 058698

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子署名装置、電子署名方法及びそのプログラムを記録した記録媒体

【特許請求の範囲】

【請求項 1】 電子的に表示される用紙に署名画像を貼り付ける電子署名装置であって、

生の署名画像を入力する署名画像入力部と、入力された生の署名画像に電子透かしを埋め込む透かし埋め込み部と、電子透かしが埋め込まれた署名画像を蓄積する埋め込み済み画像記録部とを備え、

前記透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像に埋め込むことを特徴とする電子署名装置。

【請求項 2】 前記透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込むことを特徴とする請求項 1 記載の電子署名装置。

【請求項 3】 前記画像記録部は、電子透かしが埋め込まれた署名画像を含む、用紙全体の画像を蓄積することを特徴とする請求項 1 または 2 記載の電子署名装置。

【請求項 4】 電子的に表示される用紙に署名画像を貼り付ける電子署名装置であって、

生の署名画像を入力する署名画像入力部と、入力された生の署名画像に電子透かしを埋め込む透かし埋め込み部とを備え、

前記透かし埋め込み部は、生の署名画像由来の画像を二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を施して電子透かしを埋め込み、さらに変換係数を逆二次元ウェーブレット変換して、電子透かしが埋め込まれた署名画像を生成することを特徴とする電子署名装置。

【請求項 5】 前記生の署名画像由来の画像は、生の署名画像の振幅値を定数倍したものであることを特徴とする請求項 4 記載の電子署名装置。

【請求項 6】 前記付加情報は、用紙毎にユニークに付与される識別子を含む情

報をビット展開したビット列であることを特徴とする請求項 1 又は 4 記載の電子署名装置。

【請求項 7】電子透かしが埋め込まれた署名画像から、用紙毎にユニークな付加情報を取り出す透かし取り出し部を有することを特徴とする請求項 1 又は 4 記載の電子署名装置。

【請求項 8】用紙に貼り付けられる署名画像を参照し、この署名画像が生署名画像でなく、かつ、この署名画像から前記透かし取り出し部が取り出した付加情報が正当でないとき、不正判断を行い、署名を拒否する制御部を有することを特徴とする請求項 7 記載の電子署名装置。

【請求項 9】前記署名画像は、捺印、サイン又は指紋のいずれかの画像であることを特徴とする請求項 1 から 8 記載の電子署名装置。

【請求項 10】電子的に表示される用紙に署名画像を貼り付ける電子署名方法であって、

生の署名画像に電子透かしを埋め込む透かし埋め込みステップと、電子透かしが埋め込まれた署名画像を蓄積する埋め込み済み画像記録ステップとを備え、

前記透かし埋め込みステップでは、用紙毎にユニークな付加情報を、署名画像に埋め込むことを特徴とする電子署名方法。

【請求項 11】前記透かし埋め込みステップでは、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込むことを特徴とする請求項 10 記載の電子署名方法。

【請求項 12】前記画像記録ステップは、電子透かしが埋め込まれた署名画像を含む、用紙全体の画像を蓄積することを特徴とする請求項 10 記載の電子署名方法。

【請求項 13】電子的に表示される用紙に署名画像を貼り付ける電子署名方法であって、

生の署名画像に電子透かしを埋め込む透かし埋め込みステップとを備え、

前記透かし埋め込みステップでは、生の署名画像由来の画像を二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を

施して電子透かしを埋め込み、さらに変換係数を逆二次元ウェーブレット変換して、電子透かしが埋め込まれた署名画像を生成することを特徴とする電子署名方法。

【請求項 14】前記生の署名画像由来の画像は、生の署名画像の振幅値を定数倍したものであることを特徴とする請求項 13 記載の電子署名方法。

【請求項 15】前記付加情報は、用紙毎にユニークに付与される識別子を含む情報をビット展開したビット列であることを特徴とする請求項 10 又は 13 記載の電子署名方法。

【請求項 16】電子透かしが埋め込まれた署名画像から、用紙毎にユニークな付加情報を取り出す透かし取り出しステップを有することを特徴とする請求項 10 又は 13 記載の電子署名方法。

【請求項 17】用紙に貼り付けられる署名画像を参照し、この署名画像が生の署名画像でなく、かつ、この署名画像から前記透かし取り出しステップが取り出した付加情報が正当でないとき、不正判断を行い、署名を拒否することを特徴とする請求項 16 記載の電子署名方法。

【請求項 18】前記署名画像は、捺印、サイン又は指紋のいずれかの画像であることを特徴とする請求項 10 から 17 記載の電子署名方法。

【請求項 19】生の署名画像に電子透かしを埋め込む透かし埋め込みステップと、電子透かしが埋め込まれた署名画像を蓄積する埋め込み済み画像記録ステップとを備え、

前記透かし埋め込みステップでは、用紙毎にユニークな付加情報を、署名画像に埋め込むことを特徴とする電子署名プログラムを記録した記録媒体。

【請求項 20】前記透かし埋め込みステップでは、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込むことを特徴とする請求項 19 記載の電子署名プログラムを記録した記録媒体。

【請求項 21】前記画像記録ステップは、電子透かしが埋め込まれた署名画像を含む、用紙全体の画像を蓄積することを特徴とする請求項 19 記載の電子署名プログラムを記録した記録媒体。

【請求項 22】生の署名画像に電子透かしを埋め込む透かし埋め込みステップ

とを備え、

前記透かし埋め込みステップでは、生の署名画像由来の画像を二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を施して電子透かしを埋め込み、さらに変換係数を逆二次元ウェーブレット変換して、電子透かしが埋め込まれた署名画像を生成することを特徴とする電子署名プログラムを記録した記録媒体。

【請求項 2 3】前記生の署名画像由来の画像は、生の署名画像の振幅値を定数倍したものであることを特徴とする請求項 2 2 記載の電子署名プログラムを記録した記録媒体。

【請求項 2 4】前記付加情報は、用紙毎にユニークに付与される識別子を含む情報をビット展開したビット列であることを特徴とする請求項 1 9 又は 2 2 記載の電子署名プログラムを記録した記録媒体。

【請求項 2 5】電子透かしが埋め込まれた署名画像から、用紙毎にユニークな付加情報を取り出す透かし取り出しステップを有することを特徴とする請求項 1 9 又は 2 2 記載の電子署名プログラムを記録した記録媒体。

【請求項 2 6】用紙に貼り付けられる署名画像を参照し、この署名画像が生の署名画像でなく、かつ、この署名画像から前記透かし取り出しステップが取り出した付加情報が正当でないとき、不正判断を行い、署名を拒否することを特徴とする請求項 2 6 記載の電子署名プログラムを記録した記録媒体。

【請求項 2 7】前記署名画像は、捺印、サイン又は指紋のいずれかの画像であることを特徴とする請求項 1 9 から 2 6 記載の電子署名プログラムを記録した記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、紙の用紙に、押す又は書き込んで、署名していた環境に似た環境を、電子的に実現する電子署名装置及びその関連技術に関するものである。ここで、本明細書にいう「署名」とは、一般の概念より広義であって、署名者が用紙に

記載された事項を認めるあかしとして行う行為又はこの行為の結果生ずる画像をいい、捺印、サイン、指紋を付すことなどを総称する。

【0002】

【従来の技術】

近年、オフィスでは、電子化、ペーパーレス化が進み、書類を紙に出力せず、モニターに表示するだけで、処理することが増えている。この際に問題となってくるのが、署名の取り扱いである。

【0003】

ここで、紙を用いた署名では、用紙に付された署名を、目視などで検査していた。また、用紙に付された署名を、悪意をもって、他の署名に転用することは、非常に難しい。

【0004】

しかしながら、ペーパーレスの環境下において、署名画像の情報を単にデジタル化して電子文書に貼り付けたのでは、署名画像データはデジタルであり、完全な複製を作ることができるので、署名画像データを勝手に複製し、他の文書に貼り付けるような、不正行為を簡単に行うことができる。

【0005】

このような不正行為の防止策として、「インターネットセキュリティ：佐々木良一他共著（オーム社）」120ページに、電子捺印（digital signature）に関し、次のような記述がある。

【0006】

即ち、用紙データをハッシュ関数に入力し、ハッシュ値に変換する。なお、1つのハッシュ値に対して世の中には1つの用紙しか存在しないという関係がある。そして、このハッシュ値に属性情報（電子捺印の種類を示す記号、時間情報）を結合させる。属性情報が結合されたハッシュ値を、公開鍵暗号（署名検査者の秘密鍵を使用）により変換する。この変換結果を、電子捺印とし、電子捺印付きの用紙データを次の署名検査者に送信する。この電子捺印は、秘密鍵の持ち主（この場合署名検査者）しか作成できない。

【0007】

電子捺印の検証においては、送られてきた電子捺印を送信者の公開鍵暗号により変換する。送信側での処理がすべて正しく行われたとすると、公開鍵暗号による変換結果は、送信側で生成された属性情報が結合されたハッシュ値と等しくなる。そこで、送られてきた用紙データをハッシュ関数に入力して得られたハッシュ値と、公開鍵暗号による変換結果とを比較し、ハッシュ値が一致すれば認証となる。

【0008】

【発明が解決しようとする課題】

しかしながら、上記電子捺印の技術では、署名を目視により検査する、従来の慣習から、あまりにも、かけ離れており、これに接する一般人は、違和感を禁じ得ない。

【0009】

また、電子捺印の技術は、電子取引を想定して構築されたものであり、一対一の場合には適している。しかし、用紙には、複数の署名者がそれぞれ署名を行うことも多く、これに対応するには、複数の公開鍵暗号を用意する必要があり、実用に供し難い。

【0010】

さて近年、電子透かしによって、特定のセキュリティデータを画像に埋め込む技術が実用化されているので、これを利用することも考えられる。ここで、署名の性質として、次のような点をあげることができる。

（性質1）署名は、単色（通常、白）の地に単色（赤、黒、青など）で書かれる。したがって、少なくとも輝度レベルで見ると、2値画像そのものか、それに非常に近い。

（性質2）署名の画像は、様々な用紙に繰り返し同じものが使用され、さらに同一の用紙の複数箇所に同一の署名の画像が使用されることがある。

【0011】

しかしながら、従来の電子透かしは、画像全体に目立ちにくい誤差を分散させるものばかりであり、署名の性質に合わせて特化されていない。

【0012】

即ち、従来の電子透かしによると、性質 1 に対して、2 値画像の全体に電子透かしが分散することになり、透かしが目立ちやすく、紙の用紙に署名を行った場合に比べると、見た目がかなり変わって、不自然になりやすい。

【0013】

また、性質 2 に対し、従来の電子透かしは、用紙と関係なしに、しかも、画像に依存して埋め込まれるので、同じ画像を繰り返し使用する、署名の画像では、複数の署名の画像に、同じ電子透かしが埋め込まれる可能性があり、セキュリティ上問題になりやすい。本来、従来の電子透かしは、著作権情報や商標など、用紙と全く無関係（用紙が変わっても不変）の情報を埋め込むようになっているから、このようなことになり、署名の画像には不適當なのである。

【0014】

そこで本発明は、従来の慣習に近く、かつ署名の性質に合った電子署名装置及びその関連技術を提供することを目的とする。

【0015】

【課題を解決するための手段】

本発明では、署名画像入力部から生の署名画像を入力し、入力された生の署名画像に、透かし埋め込み部が電子透かしを埋め込み、埋め込み済み画像記録部に電子透かしが埋め込まれた署名画像を蓄積するものであり、この透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像に埋め込むこととした。

【0016】

これにより、従来の慣習に近く、かつ署名の性質に合った電子署名装置を実現できる。

【0017】

【発明の実施の形態】

請求項 1 記載の発明では、生の署名画像を入力する署名画像入力部と、入力された生の署名画像に電子透かしを埋め込む透かし埋め込み部と、電子透かしが埋め込まれた署名画像を蓄積する埋め込み済み画像記録部とを備え、透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像に埋め込む。

【0018】

この構成により、生の署名画像に、電子透かしが埋め込まれ、埋め込み済み画像記録部に蓄積される。そして、埋め込まれる電子透かしは、用紙毎にユニークに付与される付加情報である。したがって、ある用紙において使用された、電子透かし埋め込み済みの署名画像を、悪意をもって他に転用しようとしても、その署名画像は、その用紙固有のものであるから、すぐに不正が露呈する。このため、同様の画像が繰り返し使用される、署名画像において、不正転用を牽制して、十分なセキュリティを確保できる。

【 0 0 1 9 】

請求項 2 記載の発明では、透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込む。

【 0 0 2 0 】

この構成によって、電子透かしは、署名画像の全体に分散して埋め込まれるのではなく、署名画像の輪郭付近に集中して、局所的に埋め込まれる。ここで、2 値画像又はそれに近い低階調の画像では、輪郭付近の変化が知覚されにくい。したがって、一般的に透かしが目立ちやすい、署名画像においても、それとわからない電子透かしを埋め込むことができ、紙の用紙に直接署名していた、従前の慣習に近く、違和感が少ない、言い換えれば、署名の性質に特化した、環境を実現できる。

【 0 0 2 1 】

請求項 3 記載の発明では、画像記録部は、電子透かしが埋め込まれた署名画像を含む、用紙全体の画像を蓄積する。

【 0 0 2 2 】

この構成により、透かし埋め込み済みの署名画像だけでなく、用紙にこれを貼り付けた画像として、蓄積するため、用紙全体のイメージを即座に、しかも簡単に取り出すことができる。また、取り出した用紙全体のイメージに含まれる署名画像を部分的に切り出して転用しようとしても、請求項 1 同様のセキュリティがあるため、このような不正を抑制できる。

【 0 0 2 3 】

請求項 4 記載の発明では、生の署名画像を入力する署名画像入力部と、入力さ

れた生の署名画像に電子透かしを埋め込む透かし埋め込み部とを備え、透かし埋め込み部は、生の署名画像由来の画像を二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を施して電子透かしを埋め込み、さらに変換係数を逆二次元ウェーブレット変換して、電子透かしが埋め込まれた署名画像を生成する。

【 0 0 2 4 】

この構成において、二次元ウェーブレット変換し、その変換係数のうち、零の値を持つ変換係数はそのままにし、非零の値を持つ変換係数に対して、用紙毎にユニークな付加情報を反映した処理を施して電子透かしを埋め込むので、署名画像の輪郭付近に電子透かしが集中して埋め込まれる。このため、請求項 2 同様の作用効果が得られるだけでなく、周波数成分により分割される各領域に対応した電子透かしを埋め込める。即ち、一又は二以上の特定の領域にのみ、電子透かしを埋め込むようにすれば、この特定の領域のみをアクセスすることで、電子透かしの抽出を、より容易にすることができる。

【 0 0 2 5 】

請求項 5 記載の発明では、生の署名画像由来の画像は、生の署名画像の振幅値を定数倍したものである。

【 0 0 2 6 】

この構成により、2 値画像又はそれに近い低階調の署名画像に対し、より知覚されにくい電子透かしを埋め込むことができる。

【 0 0 2 7 】

請求項 6 記載の発明では、付加情報は、用紙毎にユニークに付与される識別子を含む情報をビット展開したビット列である。

【 0 0 2 8 】

この構成により、小さく、軽い情報の埋め込みを行うだけで、十分なセキュリティを確保でき、かつ、演算処理負担を軽減して、処理時間を短縮することができる。しかも、生の署名画像と埋め込み画像済み署名画像との見た目の差を極力少なくすることができる。

【 0 0 2 9 】

請求項 7 記載の発明では、電子透かしが埋め込まれた署名画像から、用紙毎にユニークな付加情報を取り出す透かし取り出し部を有する。

【 0 0 3 0 】

この構成により、取り出した付加情報を利用して、不正の抑制に資することができる。

【 0 0 3 1 】

請求項 8 記載の発明では、用紙に貼り付けられる署名画像を参照し、この署名画像が生（なま）の署名画像でなく、かつ、この署名画像から透かし取り出し部が取り出した付加情報が正当でないとき、不正判断を行い、署名を拒否する制御部を有する。

【 0 0 3 2 】

この構成における、制御部により、目で見ただけでは判別困難な不正を、正確かつ高速に知ることができ、不正署名をシステム上で排除できる。

【 0 0 3 3 】

請求項 9 記載の発明では、署名画像は、捺印、サイン又は指紋のいずれかの画像である。

【 0 0 3 4 】

この構成により、現場で使用される署名画像の全てに対応できるし、一部分には捺印が使用され、他の部分にはサインが使用されるような、複数種の署名画像が混在して使用される場合にも対応できる。

【 0 0 3 5 】

次に、図面を参照しながら、本発明の実施の形態を説明する。図 1 は、本発明の一実施の形態における電子署名装置のブロック図である。図 1 に示すように、この電子署名装置は、次の構成要素を有する。まず、制御部 1 は、CPU（中央処理装置）及びそれに参照される RAM（ランダムアクセスメモリ）などからなり、電子署名装置の他の要素の動作を制御すると共に、図 5 のフローチャートに沿って、署名の正／不正判断を行い、不正と判断するときは、署名を拒否する。なお、その詳細は、後述する。

【 0 0 3 6 】

表示部 2 は、LCD や CRT 等からなり、署名者に、用紙、署名画像など、必要な情報を表示する。入力部 3 は、キーボードやマウスなどからなり、署名者がログイン ID を入力したり、その他必要な指示を与えるためのものである。

【 0 0 3 7 】

署名画像入力部 4 は、スキャナなどからなり、署名者や管理者は、これを用いて、生の署名画像を入力する。署名画像データベース 5 は、記憶装置及びこれに対して読み書きを行うデータベースエンジンからなり、入力された生の署名画像（電子透かし埋め込み前）を蓄積する。なお、署名画像データベース 5 に蓄積される、生の署名画像は、生の署名画像そのものであっても良いし、当該署名画像に係る署名権者の ID 等を電子透かしとして埋め込んだものでも良い。本明細書において、署名画像データベース 5 に蓄積される署名画像を、生の署名画像という。

【 0 0 3 8 】

用紙マスターデータベース 6 は、署名画像が貼り付けられていない、用紙（様式）の情報を蓄積する。用紙の情報は、表示部 2 に用紙の画像を表示（再現）できれば、その形式は任意であって、ラスタ系またはベクタ系の画像情報であっても良いし、HTML ファイルのようにテキスト系の情報であっても良いが、通常、ファイルやファイルの一部のフィールドとして保存される。

【 0 0 3 9 】

埋め込み情報付与部 7 は、用紙マスターデータベース 6 から作成される用紙に対して、用紙毎にユニークな付加情報を付与する。この付加情報は、用紙毎にユニークに付与される識別子を含む。こので、「用紙毎にユニーク」とは、様式が同じであっても、用紙そのものが異なれば、別個であるという意味である。単純な例を挙げると、様式 1 と様式 2 の二種類の様式が存在し、様式 1 に従う用紙が、用紙 A、用紙 B の 2 枚あり、様式 2 に従う用紙が、用紙 C、用紙 D、用紙 E の 3 枚あったとすると、用紙 A ～ 用紙 E の全てについて、互いに重複することのない、識別子が付与されることになる。このような関係を採用することによって、様式が同じ用紙間においても、署名画像の不正転用を防止できる。

【0040】

さらに、この付加情報には、他の任意の情報を追加しても良い。追加する情報としては、用紙が作成された時刻の情報や、署名者のID、用紙の様式情報などが考えられる。但し、追加する他の情報は、必要最小限にして、取り扱う情報量を小さくした方が、処理速度の点で有利であり、好ましい。

【0041】

そして、本形態では、この付加情報は、埋め込み情報付与部7によって、ビット展開され、ビット列（各ビットは、「0」か「1」）として、利用される。但し、埋め込み情報付与部7は、この付加情報を付与するだけにして、他の要素（例えば制御部1）において、ビット展開するようにしても良い。

【0042】

透かし埋め込み部8は、署名画像データベース5から、生の署名画像を入力すると共に、上記のように、ビット展開されたビット列を入力する。そして、図2のフローチャートに沿って、生の署名画像に電子透かしを埋め込み、埋め込み済み署名画像を得て、これを出力する。また、この埋め込みは、後に詳述するように、署名画像の輪郭付近に集中する。

【0043】

透かし取り出し部10は、埋め込み済み用紙データベース9に蓄積された画像から、制御部1が取り出した、埋め込み済み署名画像を入力する。そして、図4に示すフローチャートに沿って、埋め込み済み署名画像から、埋め込みビット列を取り出すと共に、埋め込み前の生の署名画像を再生し、これらビット列と生の署名画像とを出力する。

【0044】

次に、図2を用いて、透かし埋め込み部8の動作を説明する。ここで、本形態では、図3に示すような、離散ウェーブレット変換による変換係数LL、HL、LH、HHを用いる。図では、簡単のため、1階層のウェーブレット変換による変換係数を示しているが、2、3、またはそれ以上の階層としても良い。さらに、ウェーブレット変換ではなく、サブバンド分割による変換係数を用いても差し支えない。

【0045】

さて、図2に示すように、ステップ1にて、透かし埋め込み部8は、署名画像データベース5から生の署名画像を入力する。この署名画像には、発明の属する技術分野の項で述べたように、捺印、サイン、指紋などのいずれでも良く、階調や色なども任意である。但し、現実には、発明が解決しようとする課題の項において、(性質1)として指摘したように、署名画像は、ほとんど2値画像であるといっても良い。

【0046】

次に、ステップ2にて、透かし埋め込み部8は、埋め込み情報付与部7から埋め込みビット列を取得する。なお、ステップ1、2の順序は、逆にしても良い。

【0047】

ステップ3では、透かし埋め込み部8は、入力した生の署名画像に対し、その全画素の振幅値を α (1より大きい整数) 倍する。このようにすることにより、2値画像またはそれに近い、署名画像のダイナミックレンジを広くして、つまり、階調を意図的に大きくして、埋め込まれる電子透かしを、より知覚されにくくすることができる。

【0048】

次に、透かし埋め込み部8は、ステップ4にて、振幅値を α 倍した署名画像を、二次元ウェーブレット変換し、変換係数HL、LH、HHを取得する(ステップ5)。ここで、二次元ウェーブレット変換は、帯域分割フィルタとダウンサンプリングとを、適宜組み合わせれば実現できる。

なお、ここでは変換係数LLを使用しない。これは、変換係数LLを使用すると、画質劣化が顕著になるためである。また、画像の輪郭付近では、変換係数HL、LH、HHの値が大きく、変換係数HL、LH、HHを操作することにより、電子透かしを輪郭付近に集中して埋め込むことができる。

【0049】

次に、透かし埋め込み部8は、ステップ6～ステップ10の処理において、注目する変換係数Wを取り出し、埋め込みビット列による処理を施し、施した後の変換係数W' を求めてゆく。即ち、ステップ6にて、変換係数Wが零ならば、変

換係数 W をそのまま変換係数 W' とし、次の変換係数 W へ注目を移す（ステップ 10）。

【0050】

一方、変換係数 W が零でなければ、埋め込みビット列の注目ビット値を参照する（ステップ7）。このビット値が1ならば、 $W > 0$ のとき $W' = W + \beta$ 、 $W < 0$ のとき $W' = W - \beta$ とする（ステップ8）。また、このビット値が0ならば、 $W > 0$ のとき $W' = W - \beta$ 、 $W < 0$ のとき $W' = W + \beta$ とする（ステップ9）。そして、全ての変換係数 W について、以上の処理を繰り返す（ステップ10）。

【0051】

ここで、値 β は、 $8\beta < \alpha$ ($\Leftrightarrow \beta < \alpha/8$) なる条件を満たす正の整数である。これは、次の理由による。ステップ3により、画素の振幅値を α 倍したことにより、生の署名画像が n 階調とすると、振幅値のとりうる値は、

$$i\alpha \quad (i = 0, 1, 2, \dots, n-1)$$

である。

これをウェーブレット変換すると、変換係数 HL 、 LH 、 HH のとりうる値は、 $\pm i\alpha/4$ ($i = 0, 1, 2, \dots, 4(n-1)$)

である。

【0052】

つまり、変換係数同士の間隔の最小値は、 $\alpha/4$ であり、これら変換係数同士の中点までの距離は $\alpha/8$ である。したがって、上記条件 ($\beta < \alpha/8$) を満たせば、ステップ8、9の加減算を行っても、加減算後の変換係数は、この中点よりも、元の変換係数側にあることになり、加減算後の変換係数と元の変換係数とを取り違えるおそれがなくなる。逆に言えば、この条件に従っている限り、付加情報の埋め込み/取り出しが、自在に、しかも可逆的に、行えるのである。例えば、 $\beta = 1$ とするときには、 α を9以上の整数に選べば良い。

【0053】

次に、全ての変換係数 W に対する処理がすんだら、透かし埋め込み部8は、ステップ11にて、逆二次元ウェーブレット変換を行い、埋め込み済み署名画像を得て、これを出力する（ステップ12）。この逆二次元ウェーブレット変換は、

帯域合成フィルタとアップサンプラなどを適宜組み合わせれば、実現できる。

【0054】

次に、図4を用いて、透かし取り出し部10の動作を説明する。まず、透かし取り出し部10は、制御部1が埋め込み済み用紙データベース9から取り出した、埋め込み済み署名画像を入力する（ステップ20）。次に、埋め込み済みビット列を記憶する領域を初期化し（ステップ21）、埋め込み済み署名画像を二次元ウェーブレット変換して（ステップ22）、変換係数HL、LH、HHを取得する（ステップ23）。

【0055】

次に、透かし取り出し部10は、ステップ24～ステップ29の処理によって、埋め込みビット列を取り出すと共に、埋め込み前の、生の署名画像を再生する。なお、生の署名画像の再生は、省略しても良い。即ち、ステップ24にて、注目する変換係数 W' を取り出し、この変換係数 W' が零ならば、変換係数 W' をそのまま変換係数 W とし、次の変換係数 W' に注目を移す（ステップ29）。

【0056】

一方、変換係数 W' が零でなければ、ステップ25に移る。ステップ25では、まず、変換係数 W' の絶対値 A を求め、絶対値 A の $\alpha/4$ による商 K を求める。そして、次の距離 $L (= A - K\alpha/4)$ と距離 $R (= (K+1)\alpha/4 - A)$ とを求めて大小比較する。この距離 R は、絶対値 A から右側（大きい方）の $\pm i\alpha/4$ までの距離であり、距離 L は、絶対値 A から左側（小さい方）の $\pm i\alpha/4$ までの距離である。

【0057】

ここで、上述したように、 $\beta < \alpha/8$ なる条件を満たしているから、変換係数 W を $\pm\beta$ だけずらした、変換係数 W' は、隣接しうる変換係数 $W \pm \alpha/4$ よりも、元の変換係数 W に近いという関係がある。したがって、 $L < R$ なるときは、絶対値 A に対する、元の変換係数 W の絶対値は、必ず絶対値 A に近い側（左側、小さい方）にあり、図2のステップ8の処理が行われている。逆に、 $R < L$ なるときは、図2のステップ9の処理が行われている。

【0058】

このため、 $L < R$ なるとき、ステップ 27 にて、注目する埋め込みビット値を 1 とし、図 2 のステップ 8 の逆変換を行って、元の変換係数 W を得る。一方、 $R < L$ なるときは、ステップ 28 にて、注目するビット値を 0 とし、図 2 のステップ 9 の逆変換を行って、元の変換係数 W を得る。因みに、 $8\beta < \alpha$ なる条件を満たす限り、 $R = L$ となることはない。勿論、ステップ 25 の処理は、一例に過ぎず、変換係数 W' から正しく元の変換係数 W を求めることができれば、他の処理で代用しても差し支えない。

【0059】

以上の処理（ステップ 24 ～ステップ 29）を繰り返せば、埋め込みビット列を可逆的に取り出すことができ、元の変換係数 HL 、 LH 、 HH （生の署名画像に係る）の全てを再生できる。そして、透かし取り出し部 10 は、この埋め込みビット列を出力する（ステップ 30）。また、透かし取り出し部 10 は、元の変換係数を逆二次元ウェーブレット変換し（ステップ 31）、全画素の振幅値を $1/\alpha$ 倍して元に戻し（ステップ 32）、再生した生の署名画像を出力する（ステップ 33）。

【0060】

次に、図 5 を参照しながら、本形態の電子署名装置の全体動作を説明する。まず、ステップ 40 にて、制御部 1 は、表示部 2 にログオン可能表示をさせ、署名者の ID、パスワードなどの入力を求める。入力があると、制御部 1 は、署名権があるかどうかを ID 等を用いて、チェックし、署名権の確認がとれた場合のみ、次に進むことを許す（ステップ 24）。

【0061】

次に、制御部 1 は、用紙マスタデータベース 6 を参照して、表示部 2 に使用可能な用紙のリストを表示させ、署名者に使用したい用紙を選択させる（ステップ 42）。用紙が決まると、制御部 1 は、埋め込み情報付与部 7 に指示して、この用紙にユニークな埋め込みビット列を生成させる（ステップ 43）。そして、署名者に署名を行うかどうか糺す（ステップ 44）。署名しないのであれば、制御部 1 は、処理を継続するかどうか尋ね（ステップ 50）、継続するならステップ 42 へ戻り、継続しないなら終了する。

【0062】

ステップ44にて、署名者が署名を行う旨、入力部3から指示すると、制御部1は、署名画像データベース5を検索して、この署名者に関連する署名画像を表示部2にリスト表示させる。また、署名者は、リスト以外からも、例えばファイル名を指定するなどして、署名画像を指定できる（ステップ45）。

【0063】

署名画像が指定されると、制御部1は、指定された署名画像に完全に一致する画像が、署名画像データベース5に存在するかどうかチェックする（ステップ46）。もし、署名画像データベース5に存在しない署名画像が指定されていると、これは不正転用されたものである可能性がある。そこで、この場合、制御部1は、指定された署名画像を、透かし取り出し部10に渡し、図4のフローチャートに沿って、埋め込みビット列を取り出させる（ステップ51）。

【0064】

そして、制御部1は、取り出した埋め込みビット列が、ステップ43で生成したビット列と一致するかどうかチェックする（ステップ52）。もし、一致しなければ、制御部1は、指定された署名画像は不正転用されたものとして、不正判断を行い（ステップ43）、署名を拒否し、以後の入力を拒絶する。一方、ステップ52で一致を見れば、制御部1は、署名画像は正当として、ステップ48へ移る。

【0065】

ここで、ステップ52において、一致となるのは、同じ用紙に同じ署名画像を複数使うような場合である。即ち、一つの署名が正当に行われた後、この署名画像をコピー&ペーストして、同じ用紙の他の箇所へ用いると、一致となる。このようなときは、最初の署名時に正当性をチェックしてあるから、署名画像の同一用紙内の転用を認めても、差し支えない。

【0066】

さて、ステップ46にて、署名画像データベース5に完全に一致する画像が見つかり、制御部1は、生の署名画像が正当に指定されたものと判断し、透かし埋め込み部8へ指示して、図2のフローチャートに沿って、埋め込みビット列を

電子透かしとして埋め込ませ、埋め込み済み署名画像を得る（ステップ47）。そして、制御部1は、埋め込み済み署名画像を用紙の所定領域に貼り付けた画像を生成して、表示部2を介して署名者に提示すると共に、この画像を埋め込み済み用紙データベース9に保存させる（ステップ48、49）。そして、制御部1は、以上の処理を、継続が希望されるだけ（ステップ50）、繰り返す。

【0067】

以上の説明により、単一人の署名だけでなく、各人が次々に署名を行えることが容易に理解されよう。

【0068】

次に、図6～図10を用いて、本形態の電子署名装置による署名例を説明する。まず図6～図9は、用紙の例として、稟議書を示している。図6に示すように、この稟議書は、右上部に「起案者」、「課長」、「部長」、「本部長」、「社長」のそれぞれが、署名（この例では捺印）すべき、矩形の捺印欄が設けてあり、図示した状態では、既に、「起案者」（山口）、「課長」（田中）が捺印を済ませ、「部長」が捺印したばかりのところである。そして、「部長」は、鈴木某であり、彼の生の署名画像を拡大すると、図7のようになる。

【0069】

また、ここでは、「19990726103297863」という、付加情報が設定され、これをビット展開したビット列が、埋め込みビット列とされる。因みに、「199907261032」なる数字は、1999年7月26日10時32分という、用紙作成時間であり、「97863」なる数字は、この稟議書の識別子である。勿論、これは一例に過ぎず、付加情報は種々設定できるし、図示しているように、付加情報を表示する必要はないことは、いうまでもない。

【0070】

さて、図7の生の署名画像に対して、上記ビット列を埋め込む電子透かし（図2のフローチャートに準拠）だけを取り出して図示すると、図8のようになる。図7と図8とを比べれば、この電子透かしは、輪郭付近に集中していることは、明らかであろう。このようにすると、人間の視覚特性から、2値画像またはそれに近い、署名画像であっても、極めて知覚されにくい、電子透かしを埋め込むこ

とができる。その証拠に、埋め込み済み署名画像を図 9 に示しているが、図 7 と図 9 とを目視で比較しても、その差異を見つけることは、ほとんど不可能である。因みに、図 6 の捺印欄には、埋め込み済み署名画像（「部長」の捺印欄には、図 7 ではなく図 9 の画像）が表示される。

【 0 0 7 1 】

また、この例では、捺印を取り扱ったが、署名画像を包囲する領域（図 6 では、捺印欄）の形状やサイズを適宜変更すれば、図 1 0 に示すような、サインを用いる場合や、指紋などにも、本発明は、同様に適用できる。さらには、捺印、サイン、指紋などが混在する状態で使用される場合にも、同様に対応できる。

【 0 0 7 2 】

ここで、本明細書にいう「電子署名プログラムをコンピュータ読み取り可能に記録した記録媒体」には、複数の記録媒体にプログラムを分散して配布する場合を含む。また、このプログラムが、オペレーティングシステムの一部であるか否かを問わず、種々のプロセスないしスレッド（DLL、OCX、ActiveX 等（マイクロソフト社の商標を含む））に機能の一部を肩代わりさせている場合には、肩代わりさせた機能に係る部分が、記録媒体に格納されていない場合も含む。

【 0 0 7 3 】

図 1 には、スタンドアロン形式のシステムを例示したが、サーバー／クライアント形式にしても良い。つまり、1 つの端末機のみ、本明細書に出現する全ての要素が含まれている場合の他、1 つの端末機がクライアントであり、これが接続可能なサーバないしネットワーク上に、全部又は一部の要素が実存していても、差し支えない。

【 0 0 7 4 】

さらには、図 1 のほとんどの要素をサーバー側で持ち、クライアント側では、例えば、WWWブラウザだけにしても良い。この場合、各種の情報は、通常サーバ上にあり、基本的にネットワークを経由してクライアントに配布されるものだが、必要な情報が、サーバ上にあるときは、そのサーバの記憶装置が、ここにいる「記録媒体」となり、クライアント上にあるときは、そのクライアントの記録

装置が、ここにいう「記録媒体」となる。

【0075】

さらに、この「電子署名プログラム」には、コンパイルされて機械語になったアプリケーションの他、上述のプロセスないしスレッドにより解釈される中間コードとして実存する場合や、少なくともリソースとソースコードとが「記録媒体」上に格納され、これらから機械語のアプリケーションを生成できるコンパイラ及びリンカが「記録媒体」にある場合や、少なくともリソースとソースコードとが「記録媒体」上に格納され、これらから中間コードのアプリケーションを生成できるインタプリタが「記録媒体」にある場合なども含む。

【0076】

【発明の効果】

請求項 1、10、19 では、用紙固有の電子透かしを用いて、署名画像の不正転用を防止できる。

【0077】

請求項 2、11、20 では、極めて知覚されにくい電子透かしとすることができ、従前の慣習に近く、違和感が少ない、環境を提供できる。

【0078】

請求項 3、12、21 では、用紙全体のイメージを、簡単に取り出せる。

【0079】

請求項 4、13 では、知覚されにくい電子透かしを、周波数領域に分けて埋め込める。

【0080】

請求項 5、14、22 では、2 値画像又はそれに近い低階調の署名画像に対し、より知覚されにくい電子透かしを埋め込める。

【0081】

請求項 6、15、23 では、十分なセキュリティと、処理速度とを両立できる。

【0082】

請求項 7、16、24 では、取り出した付加情報を利用して、不正を抑制でき

る。

【 0 0 8 3 】

請求項 8、1 7、2 5 では、不正署名をシステム上で排除できる。

【 0 0 8 4 】

請求項 9、1 8、2 6 では、様々な署名画像に対応できる。

【図面の簡単な説明】

【図 1】

本発明の一実施の形態における電子署名装置のブロック図

【図 2】

同透かし埋め込み部のフローチャート

【図 3】

同変換係数の説明図

【図 4】

同透かし取り出し部のフローチャート

【図 5】

同電子署名装置のフローチャート

【図 6】

同捺印を用いる用紙の例示図

【図 7】

同生の署名画像の拡大図

【図 8】

同電子透かしの拡大図

【図 9】

同埋め込み済み署名画像の拡大図

【図 1 0】

同サインを用いる用紙の例示図

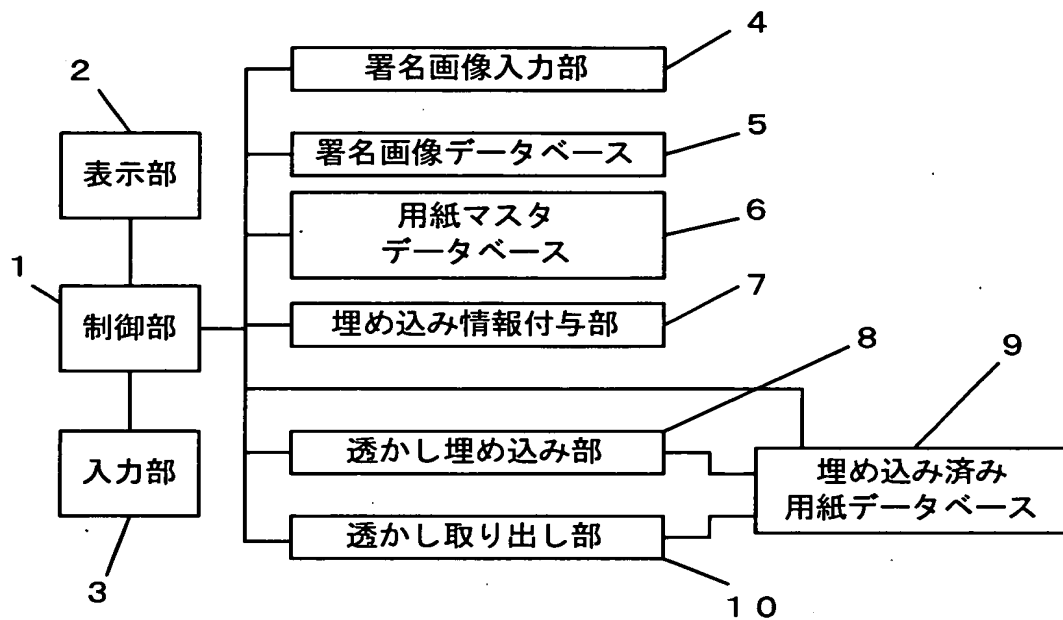
【符号の説明】

- 1 制御部
- 2 表示部

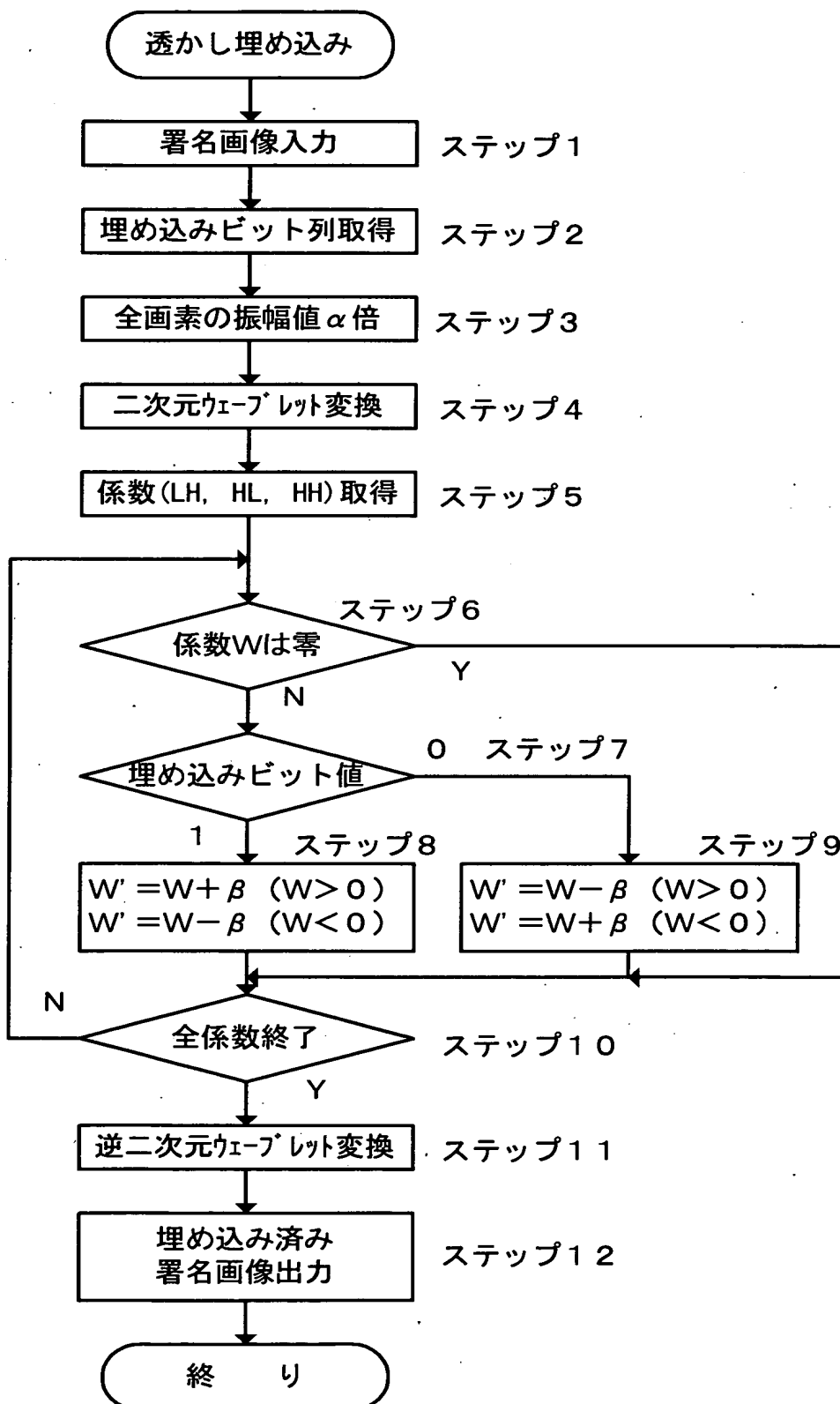
- 3 入力部
 - 4 署名画像入力部
 - 5 署名画像データベース
 - 6 用紙マスターデータベース
 - 7 埋め込み情報付与部
 - 8 透かし埋め込み部
 - 9 埋め込み済み用紙データベース
 - 1 0 透かし取り出し部
- H L、L H、H H 変換係数

【書類名】 図面

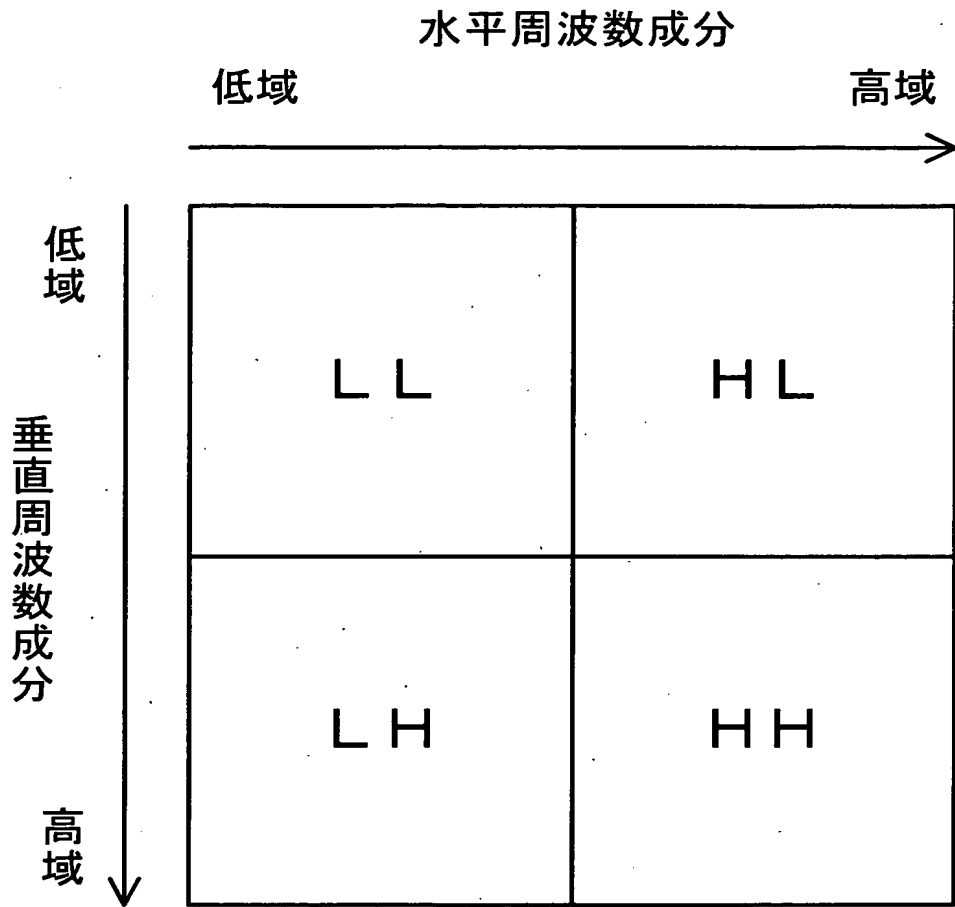
【図 1】



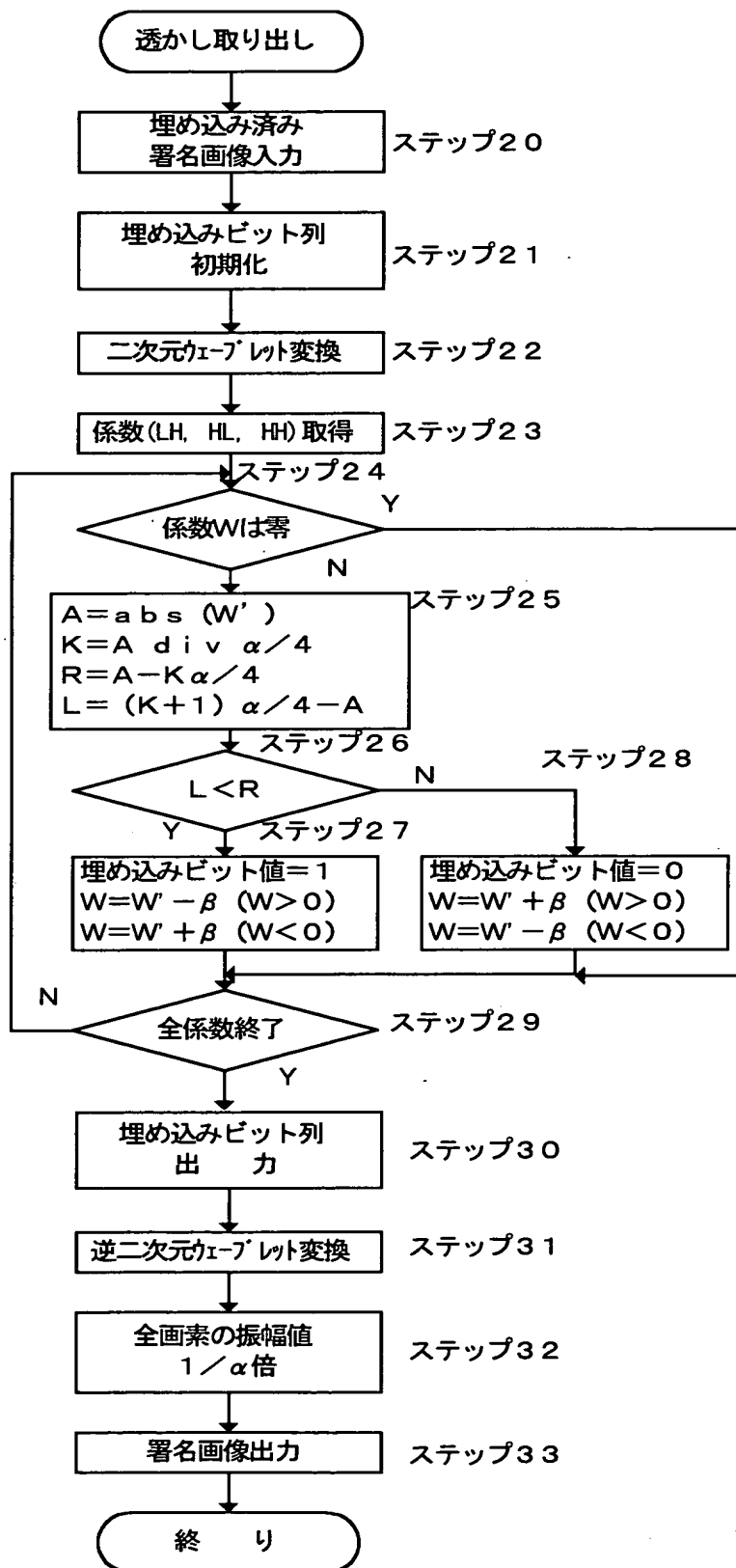
【図 2】



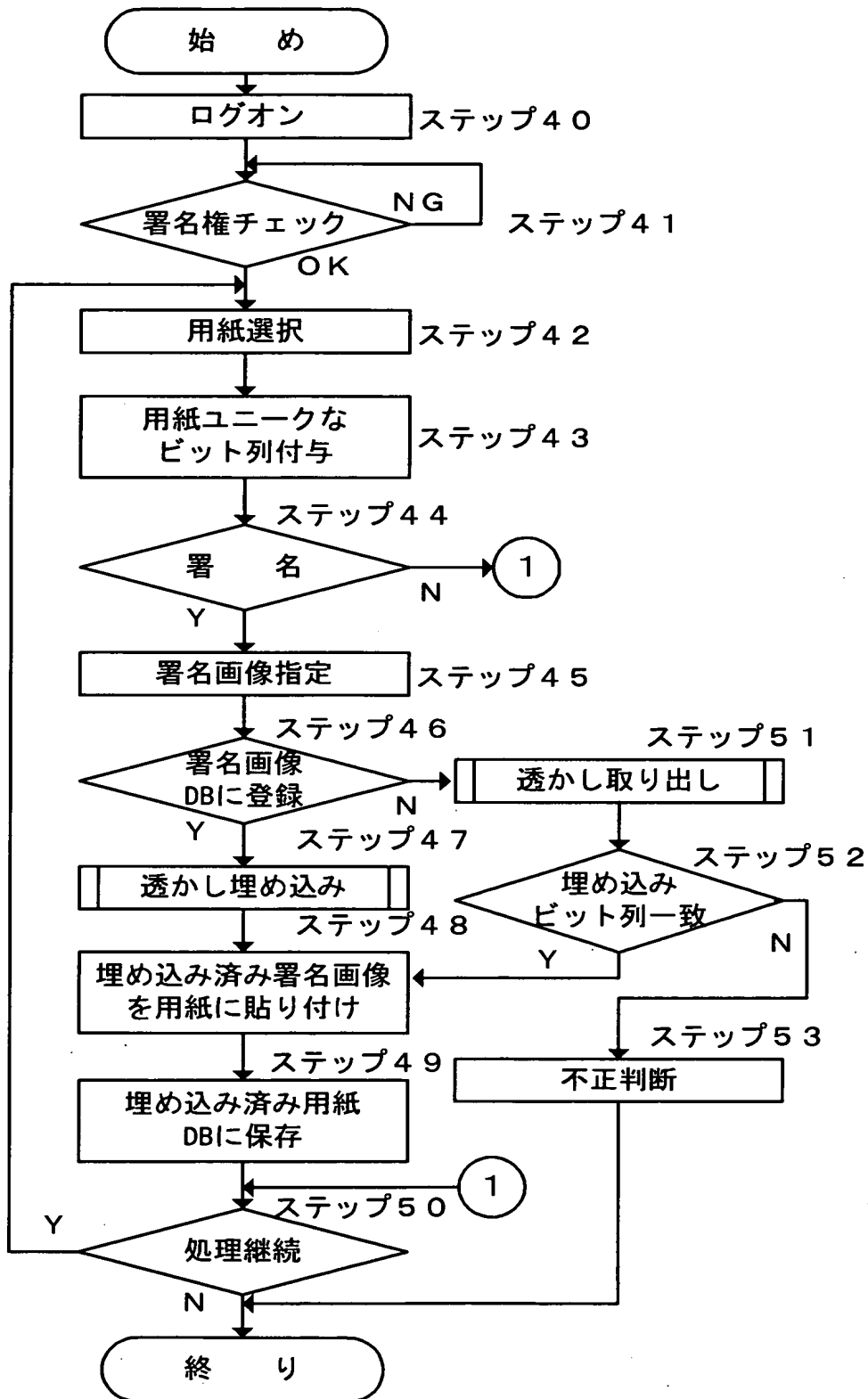
【図 3】



【図 4】



【図 5】

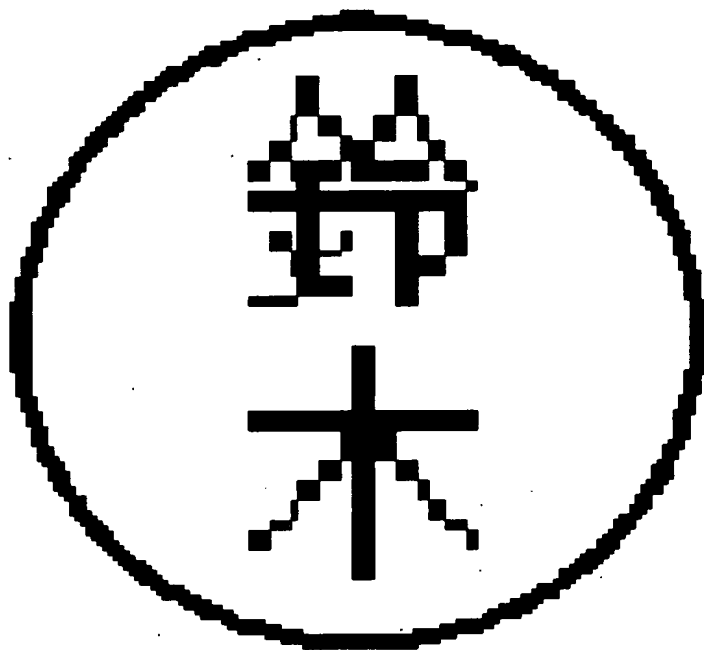


【図 6】

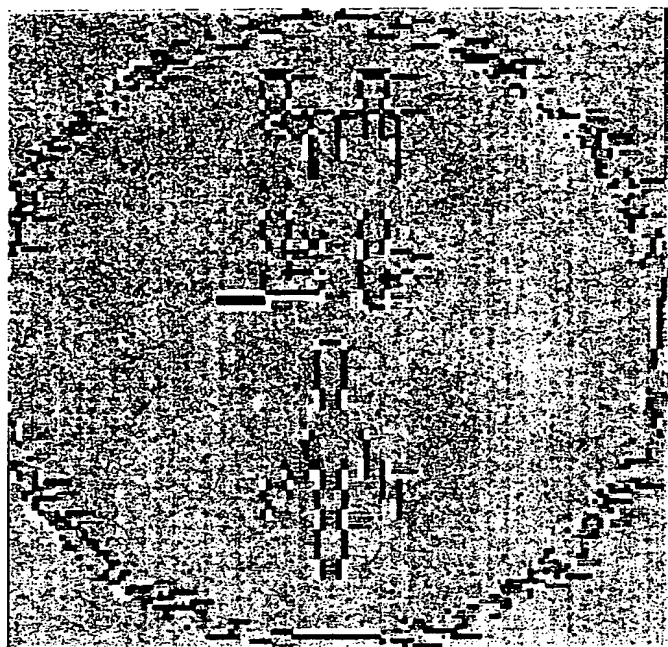
<1990726103297863>					
稟議書	社 長	本部長	部 長	課 長	起案者
			<div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> 鈴木 </div>	<div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> 田中 </div>	<div style="border: 1px solid black; border-radius: 50%; width: 40px; height: 40px; margin: 0 auto; display: flex; align-items: center; justify-content: center;"> 山口 </div>

件名		文書番号	稟第 1 2 3 4 号
		起 案 日	1999年 7月26日
		決 裁 日	年 月 日

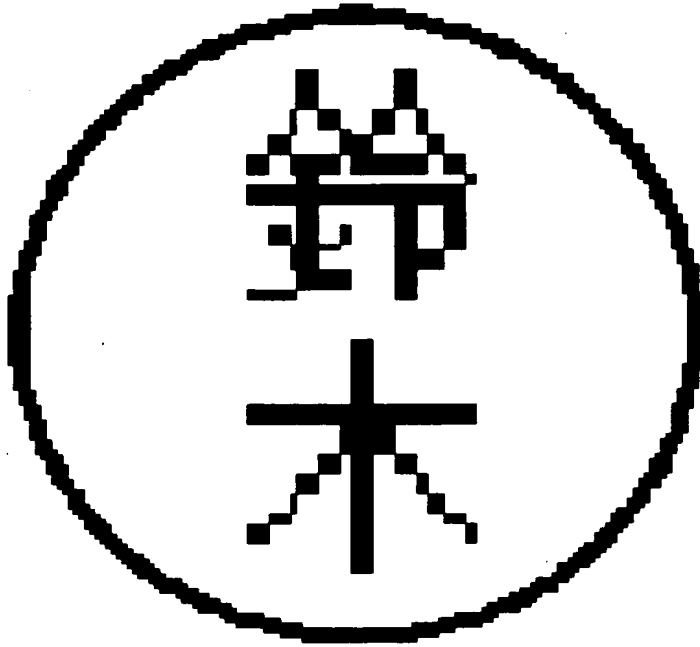
【図 7】



【図 8】



【図 9】



【図 10】

Signature:	<u>Taro Matsushita</u>
Date :	<u>July 26, 1999</u>
<1990726103297864>	

【書類名】 要約書

【要約】

【課題】 従来の慣習に近く、署名の性質に合った電子署名装置を提供する。

【解決手段】 署名画像入力部 4 から生の署名画像を入力する。入力された生の署名画像に、透かし埋め込み部 8 が電子透かしを埋め込み、埋め込み済み用紙データベース 9 に、電子透かしが埋め込まれた署名画像を蓄積する。透かし埋め込み部は、用紙毎にユニークな付加情報を、署名画像の輪郭付近に集中して埋め込む。2 値画像に近い署名画像においても、電子透かしは、極めて知覚されにくく、しかも、署名画像の不正転用を防止できる。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社